national education union

Social Media and Online Safety – Advice for School Staff
NEU guidance for members in England, Wales & Northern Ireland

The purpose of this document is to advise NEU members how to stay safe online and protect their online reputation. It also provides information about commonly used social media sites and how their misuse might have implications in schools and colleges.

What we say
When you read through this document you may have questions about what happens in your particular school or workplace, and there may be collective issues that affect other members. In most circumstances, you should initially discuss the matter with your workplace rep, as they will know whether similar concerns have been raised by other members. If you do not have a rep at the moment, it would be a good idea to get members together to elect one. Further advice on this is available at: neu.org.uk/becoming-a-rep

Although you may sometimes feel that you are the only person affected by or concerned about a particular issue, in reality this is seldom the case. Any difficulties you may experience are likely to be linked to wider conditions at your workplace and as a member of the NEU you have the advantage of being able to act collectively with your colleagues. This should give you the confidence of knowing that you have the weight of the union behind you.

Why is online safety an issue for schools?
Social media, or social networking, sites are abundant, used by young people and adults alike.

School staff need to be aware of online safety issues, both in relation to themselves and pupils. For instance, school staff need to be aware of their online reputation, and may be victims of cyberbullying perpetrated within the school community. Similarly, pupils can be victims or perpetrators of cyberbullying, or be involved in ‘sexting’ incidents. School employers have a legal requirement to protect their workers from abuse and bullying online, in the same way as face-to-face bullying. Schools are also required to teach children and young people about online safety issues.

What different types of social networks are there?
Some commonly used social media sites are listed below. Most sites have a minimum age for users to be eligible to use the service; however, evidence shows that children younger than these limits are accessing social media sites, often because the sites do not ask for confirmation of age at sign up.

- Facebook (minimum age 13) – lets users create their own profiles, share status updates, pictures, videos and chat with other users, and also has a messenger app.

- Instagram (minimum age 13) – allows users to alter photos, upload them to Instagram and share them to other social networking sites. Photos can be sent directly to specific users. A video feature is also available.
- Snapchat (minimum age 13) – a photo-sharing app where users can send photos or videos to their friends. These will display on screen for up to ten seconds before being deleted, although it is possible to take screenshots of messages and download other apps designed to capture and save Snapchat content.
- Twitter (minimum age 13) – a social network that lets users send and read 'tweets', messages limited to 280 characters.
- Tumblr (minimum age 16) – a social networking site where users can post blogs and follow other people's blogs. Some of the content on this site contains sexual or pornographic images.
- WhatsApp (minimum age 16) – free-of-charge, real-time messaging. Users can share images and videos, take part in 'group chats' and share locations. As it's based on knowing the user's phone number, you can only message users if you already know their telephone number.
- YouTube (minimum age 13) – allows users to watch, create and comment on videos.
- ASKfm (minimum age 13) – users can ask other users questions, with the option of anonymity. ASKfm's reputation as a platform for cyberbullying has been highlighted in the media.

The Safer Internet Centre and the NSPCC Net Aware websites have guides on these and other types of social media, including details of terms and conditions of usage and safety tools (see further information, below).

What are the potential uses and misuses of social media in a school setting?
Using the internet appropriately with children and young people can be a useful and rewarding resource for teachers and school staff. Many young people use social media safely and suitably. However, the proliferation of social media presents a number of issues that have the potential to affect school staff and pupils negatively.

It is important for teachers and school staff to be aware of their online reputation and recognise that their online activity can be seen by others on social media. This potentially includes wider groups of people than those befriended on social media – and therefore, it is vital that school staff who use social media apply strong privacy settings. Advice for school staff on staying safe online is detailed below in the next section.

Cyberbullying is the use of technologies, such as social networking, to deliberately and repeatedly upset someone else. School staff are known to have been victims of cyberbullying, and in fact, the Department for Education (DfE) says that 21 per cent of teachers have reported having derogatory comments posted about them on social media by parents and/or pupils. Pupils can be victims and perpetrators of cyberbullying. Schools should have a policy on cyberbullying and should make it clear to all members of the school community that like face-to-face bullying, cyberbullying will not be tolerated.

Sexting is another issue that may need to be addressed at school level. It is a broad term, but for the purposes of NEU guidance to schools, it is used to refer to “images or videos generated by children under the age of 18, or of children under the age of 18 that are of a sexual nature, or are indecent”. Sometimes such behaviour can be part of a romantic relationship between young people; however, it can also be coercive and/or exploitative, and images can be used to bully and blackmail children and young people. Comprehensive NEU self-help guidance on sexting is available in the self-help section of the website.

How can I protect myself and my reputation online?

The nature of teaching and working in education means that school staff need to be particularly aware of their online reputation, including information posted about them by others. While the NEU does not advise members against using social media for personal use, it does advise them to think carefully about the way they use these technologies.

There have been cases of school employees being subject to disciplinary action because of things that have been posted online.

Below is NEU advice for school staff on how to stay safe online and when using technology and social media:

- Review your privacy settings, and ensure that they are sufficiently robust. Sites such as Facebook allow you to view your page as different groups of people, eg friends, non-friends.
- Privacy tools that are available on many social media sites include: customising who can see your posts; controlling who can contact you and make ‘friend’ requests; keeping your location private; and approving tags before they are published.
- Discuss expectations around tagging posts with friends and family. For instance, you may prefer to not be tagged in any posts on social media.
- Regularly search your name in search engines and social media sites to check what information there is on the internet about you. It is standard practice for employers to search prospective employees online, so search yourself online when applying for any posts. When searching, check variations of your name and even nicknames.
- If offensive or hurtful information is posted about you online, for instance, by a pupil or parent, never retaliate to the message. There have been cases where school staff have been disciplined by their employer for responding to posts online, even where they were not the instigator. Instead, make copies of all offensive content, including screenshots and URLs, and take them to your employer. Your employer must take action on cyberbullying in the same way as it would face-to-face bullying.

- If offensive material has been posted about you online, you can use the reporting procedures of the site involved to get the material taken down. More information on how to do this is available in the NEU self-help briefing on cyberbullying.
- Make sure you have familiarised yourself with your employer's IT 'acceptable use' policy and abide by the requirements of this policy. For instance, if you access personal email and social media accounts when connected to the employer's Wi-Fi network, these may be subject to the school's internet policy which is likely to include monitoring and surveillance.
- Only use work equipment and email for work uses – and do not let anyone else, including colleagues and family members, use them.
- Ensure all of your devices, including work ones, are password protected. Do not give your password to anyone else and do not leave your screen unlocked if you move away from the device.
- Do not befriend any current pupils on social media – it is likely to be in breach of your employer's policies. If pupils are consistently attempting to 'friend' you on social media, report this to your employer.
- While former pupils may not be covered by your employer's policy, NEU advice is to very carefully consider the implications of befriending former pupils, especially as they may have friends, siblings or connections to current pupils. Similarly, there are potential implications of befriending parents of pupils on social media – even if they are also a colleague. Therefore, it is recommended that NEU members do not friend former pupils or parents on social media. If you do decide to do this, let your employer know.
- Keep your personal phone number private and do not share with pupils or parents. If it is necessary to use a mobile phone to contact parents, eg during a school trip, your employer must provide one.
- Be aware that your employer will be able to check your usage and data, including location history, on any device they provide you for work purposes. (Details of how to turn off location settings on iPhone is available in the NEU health and safety briefing on online safety.)
- When using social media, before posting or commenting on items, consider whether you would be happy for your employer, colleagues, pupils and parents to see it. If you wouldn't want them to, then don't post it online.
- Never criticise your school, employer, pupils or parents online.

Childnet has produced a social media guide for teachers and support staff. The UK Safer Internet Centre runs an online safety helpline for professionals, and it can provide advice to school staff with queries or concerns about all sorts of online safety issues. It can be contacted on 0344 381 4772 or helpline@saferinternet.org.uk

What can I expect from my employer?
Your employer should have policies addressing various online safety issues including: IT acceptable usage (for staff and pupils), cyberbullying, sexting, and appropriate use of social media. They should be communicated to all staff, pupils and parents, and refer to other policies, such as pupil behaviour and safeguarding, where relevant. The policies

should set out clear reporting procedures and who the lead is in the school on online safety, ie a member of the senior management team (SMT). The policy should also list the potential sanctions that can be employed if there a breach of the policy, including for pupils, parents and staff.

Where a member of staff is the victim of cyberbullying, the NEU expects the school to respond as thoroughly as it would to any other types of bullying, including taking steps to support the member of staff to get the offensive material taken off the internet.

What support should schools provide pupils in relation to online safety?
The DfE statutory guidance for schools and colleges, Keeping children safe in education, states that "governing bodies and proprietors should be doing all that they reasonably can to limit children's exposure to…risks from the school's or college's IT system". This includes ensuring that the school/college has appropriate filters and monitoring systems in place.

The Safer Internet Centre has guidance for schools on appropriate filtering and monitoring. The DfE advises that there should be a whole school approach to online safety and that online safety training for staff is integrated, aligned and considered as part of the overarching safeguarding approach.

The UK Council for Child Internet Safety (UKCCIS) has produced a framework to support schools in teaching pupils about online and digital issues.

The Government has also stated that the reforms to Relationships Education (primary schools) and Relationships and Sex Education (secondary schools), which include making the subjects mandatory, will include a key focus on "healthy relationships and safety online, including use of social media, cyberbullying and sexting".

What should I do next?
If further advice is needed, contact your NEU workplace rep in the first instance. If there is no NEU rep in your workplace, or the peripatetic nature of your employment makes contact with a workplace rep difficult, contact the NEU Adviceline in England on 0345 811 8111, NEU Cymru in Wales on 029 2046 5000 or NEU Northern Ireland on 028 9078 2020.
Further contact details may be found at: neu.org.uk/contact-us

Further information
Childnet International – offers advice for professionals on online safety issues affecting young people.
childnet.com/teachers-and-professionals/for-working-with-young-people/hot-topics

UK Safer Internet Centre
saferinternet.org.uk/advice-centre/teachers-and-school-staff/appropriate-filtering-and-monitoring

DfE – Keeping children safe in education
gov.uk/government/publications/keeping-children-safe-in-education--2

NEU guidance
Available at neu.org.uk
Cyberbullying – self-help guidance
Sexting – self-help guidance
Discrimination and harassment – self-help guidance
Online safety – health and safety guidance and model policy for reps and local officers
Bullying and harassment - health and safety guidance and model policy for reps and local officers